

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN RE APPLICATION OF THE UNITED
STATES OF AMERICA FOR AN ORDER
AUTHORIZING THE INSTALLATION
AND USE OF PEN REGISTERS AND
TRAP AND TRACE DEVICES FOR

CELL PHONE NUMBER: 614-756-9477

Misc. No. 2:18-mj-796

Filed Under Seal

APPLICATION

The United States of America, moving by and through Assistant United States Attorney Jessica H. Kim, its undersigned counsel, respectfully submits under seal this *ex parte* application for an order pursuant to 18 U.S.C §§ 3122 and 3123 that authorizes the installation and use of pen registers and trap and trace devices (“pen-trap devices”) to record, decode, and/or capture dialing, routing, addressing, and signaling information for communications to or from the cellular telephone number described in Attachment A, including the date, time, and duration of the communication and those items listed in Attachment B, without geographic limit. In support of this application, the United States asserts:

1. This is an application, made under 18 U.S.C. § 3122(a)(1), for an order under 18 U.S.C. § 3123 authorizing the installation and use of a pen register and a trap and trace device.
2. Such an application must include three elements: (1) “the identity of the attorney for the Government or the State law enforcement or investigative officer making the application”; (2) “the identity of the law enforcement agency conducting the investigation”; and (3) “a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.” 18 U.S.C. § 3122(b).

3. The undersigned applicant is an “attorney for the government” as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure.

4. The law enforcement agency conducting the investigation is the Federal Bureau of Investigation (“FBI”).

5. The applicant hereby certifies that the information likely to be obtained by the requested pen-trap devices is relevant to an ongoing criminal investigation being conducted by the FBI.

6. This Court is a “court of competent jurisdiction” under 18 U.S.C. § 3122(a)(2) because it “has jurisdiction over the offense being investigated.” 18 U.S.C. § 3127(2)(A)(i).

ADDITIONAL INFORMATION

7. Other than the three elements described above, federal law does not require that an application for an order authorizing the installation and use of a pen register and a trap and trace device specify any facts. The following additional information is provided to demonstrate that the order requested falls within this Court’s authority to authorize the installation and use of a pen register or trap and trace device under 18 U.S.C. § 3123(a)(1).

8. A “pen register” is “a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted.” 18 U.S.C. § 3127(3). A “trap and trace device” is “a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication.” 18 U.S.C. § 3127(4).

9. In the traditional telephone context, pen registers captured the destination phone numbers of outgoing calls, while trap and trace devices captured the phone numbers of incoming calls. Similar principles apply to other kinds of wire and electronic communications, as described below.

10. A cellular telephone, or cell phone, is a mobile device that can transmit and receive both wire and electronic communications. Individuals using cell phones contract with cellular service providers that maintain antenna towers (also known as cell towers) covering specific geographic areas. In order to transmit or receive calls and data, a cell phone must send a radio signal to a cell tower that, in turn, is connected to a cellular service provider's network. A cell phone connected to a cellular service provider's network can thus act much like a traditional landline telephone and a computer.

11. This application seeks authorization to install and use pen-trap devices to record, decode, and/or capture dialing, routing, addressing and signaling information related to electronic communications and to traditional calls and messages sent to and from the cell phone number described in Attachment A.

ELECTRONIC COMMUNICATIONS DATA

12. The Internet is a global network of computers and other devices. Cell phones can connect to the Internet via the cellular network and then be used to browse the World Wide Web, send e-mail messages, and engage in other forms of electronic communications, just like desktop and laptop computers.

13. In order to connect to the Internet via the cellular network, a cell phone must first connect to a cell tower. Each cell phone has one or more unique identifiers embedded inside it that it reveals to the cell tower when making this connection; the cell tower receives and

forwards those identifiers to the core network as a matter of course. Examples of these unique identifiers include an Electronic Serial Number (“ESN”), a Mobile Equipment Identifier (“MEID”), or an International Mobile Station Equipment Identity (“IMEI”). Depending on the cellular network and the device, a cell phone may also have a Subscriber Identity Module (“SIM card”) that contains additional identifiers, including an International Mobile Subscriber Identity (“IMSI”). The unique identifiers – as transmitted from a cell phone to a cellular network – are similar to telephone numbers in that they are used by the cellular provider to identify, authenticate, and/or route the communications. They can be recorded by pen-trap devices and indicate the identity of the cell phone device making the communication without revealing the communication’s content.

14. On the Internet, data transferred between devices is not sent as a continuous stream, but rather it is split into discrete packets. Generally, a single communication is sent as a series of data packets. When the packets reach their destination, the receiving device reassembles them into the complete communication. Each packet has two parts: a header with routing and control information and a payload, which generally contains the content of the transmitted communication.

15. The packet header contains non-content dialing, routing, addressing, and signaling information, including Internet Protocol (“IP”) addresses and port numbers. Both the IP address of the requesting device (“the source IP address”) and the IP address of the receiving device (“the destination IP address”) are included in specific fields within the packet header, as are source and destination port numbers. On the Internet, IP addresses and port numbers function much like telephone numbers and area codes – often both are necessary to route a communication.

16. IP addresses are unique identifiers that are assigned to each device directly connected to the Internet and that are used to route information between devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response.

17. Port numbers can serve different functions. Sometimes, port numbers identify the type of service, such as email or web browsing, associated with a communication. For example, port 80 is typically associated with communications relating to browsing web pages. In other cases, port numbers are used to specify a specific device on a private network to which or from which communications are sent. In either case, port numbers are used to route data packets either to a specific device or to a specific process running on a device. Thus, in both cases, port numbers are used by computers to route data packets to their final destinations.

18. The headers of data packets also contain other dialing, routing, addressing, and signaling information. This information includes the transport protocol used (there are several different protocols that govern how data is transferred over networks); the flow label (for the most recent version of the Internet Protocol suite known as IPv6, the flow label helps control the path and order of transmission of packets); and the packet size.

19. Because they are all used to facilitate the routing and transfer of data, and because they do not contain the content of communications, the United States requests that this Court order **AT&T** to either produce, or assist the United States in obtaining through the installation of a pen-trap device, IP addresses, port numbers, transport protocol, flow label, and packet size of each data packet sent to and from the cell phone number described in Attachment A, as well as the unique cell phone identifiers, described above, associated with each such electronic communication. See 18 U.S.C. §§ 3122 and 3123.

20. The United States further requests that the Court order **AT&T** to provide other data related to each data packet sent over the provider's network. These data fields are commonly provided by cellular telephone providers pursuant to industry standards adopted under the Communications Assistance for Law Enforcement Act (CALEA). See 47 U.S.C. § 1006. They include: the Case Identification (or Case ID), which is a unique identifier used by law enforcement and the provider to identify the case to which the data pertains; the Intercept Access Point System Identification (IAP System ID), which identifies the network equipment responsible for isolating the targeted information; the Timestamp, which identifies the date and time that the event was detected; and the Correlation Number, which provides a unique identifier for the data that is used to correlate the communication identifying information with the communication content.

TRADITIONAL CALLING AND MESSAGING DATA

21. Pen-trap devices can record the telephone numbers with which a cell phone corresponds by placing or receiving telephone calls or by placing and receiving Short Message Service ("SMS") and Multimedia Message Service ("MMS") messages (which may include text, photographs, videos, and other data). These telephone numbers can then be used to identify the parties to a communication without revealing the communication's content.

22. These telephone numbers can include "post-cut-through-dialed-digits," which are numbers dialed from the cell phone after the initial call set up is completed. For example, some post-cut-through-dialed digits may be the actual telephone number called, such as when a subject places a calling card, credit card, or collect call by first dialing an access number and then, after the initial call is "cut-through," dialing the telephone number of the destination party. That final number sequence is necessary to route the call to the intended party and, therefore, identifies the

place or party to which the call is being made. In the event that the pen-trap devices capture some post-cut-through-dialed digits that could be considered call content, such as account numbers or passwords, despite the government's use of reasonably available technology to avoid the recording or decoding of such content, the United States will make no affirmative investigative use of such information.

23. In order to send or receive calls or messages via the cellular network, a cell phone must first connect to a cell tower. In doing so, it reveals one or more of the unique identifiers embedded inside it to the cell tower, which records and forwards this information to the core network as a matter of course. As explained above, these unique identifiers include an Electronic Serial Number, a Mobile Equipment Identifier, an International Mobile Station Equipment Identity, and an International Mobile Subscriber Identity, and these identifiers are used by the cellular provider to identify, authenticate, and/or route the communications. They can be recorded by pen-trap devices and indicate the identity of the cell phone device making the communication without revealing the communication's content.

24. Because they are all used to facilitate the routing and transfer of communications, and because they do not contain the content of communications, the United States requests that this Court order **AT&T** to either produce, or assist the United States in obtaining through the installation of a pen-trap device, the telephone number and other unique identifiers, such as those described above, relating to each call and SMS/MMS message sent to and from the cell phone described in Attachment A. See 18 U.S.C. §§ 3122 and 3123.

THE RELEVANT FACTS

25. The United States government, including the FBI, is investigating possible police corruption. The investigation concerns possible violations by Columbus Division of Police

(“CPD”) Officer Steven G. Rosser, among others. The investigation concerns possible violations of, *inter alia*, 18 U.S.C. § 242 (deprivation of rights under color of law) and 18 U.S.C. 1951 (Hobbs Act extortion).

26. The investigation relates to possible police corruption. Investigators believe that matters relevant to the offenses under investigation have been and continue to be discussed using **AT&T** cell phone number **614-756-9477**. **AT&T** is an electronic communication service provider doing business in **North Palm Beach, FL**. Investigators believe that the listed subscriber for this number is Columbus Division of Police Officer Steven G. Rosser, a target of this investigation.

27. The conduct being investigated involves use of the cellular telephone number described in Attachment A. To further the investigation, investigators need to obtain the dialing, routing, addressing, and signaling information associated with communications sent to or from that cell phone number.

28. The pen-trap devices sought by this application will record, decode, and/or capture dialing, routing, addressing, and signaling information for all calls, SMS messages, and MMS messages, as well as all data packets associated with each electronic communication sent via the Internet to or from the cell phone number described in Attachment A, including the date, time, and duration of the communication and those items listed in Attachment B, without geographic limit.

GOVERNMENT REQUESTS

29. For the reasons stated above, the United States requests that the Court enter an Order authorizing the installation and use of pen-trap devices to record, decode, and/or capture the dialing, routing, addressing, and signaling information for all calls, SMS messages, and

MMS messages, as well as all data packets associated with each electronic communication sent to or from the cell phone number described in Attachment A, including the date, time, and duration of the communication and those items listed in Attachment B, without geographic limit. The United States does not request and does not seek to obtain the contents of any communications, as defined in 18 U.S.C. § 2510(8).

30. The United States further requests that the Court authorize the foregoing installation and use for a period of sixty days from the date of the Court's Order, pursuant to 18 U.S.C. § 3123(c)(1).

31. The United States further requests, pursuant to 18 U.S.C. §§ 3123(b)(2) and 3124(a)-(b), that the Court order **AT&T** and any other person or entity providing wire or electronic communication service in the United States whose assistance may facilitate execution of this Order to furnish, upon service of the Order, information, facilities, and technical assistance necessary to install the pen-trap devices, including installation and operation of the pen-trap devices unobtrusively and with minimum disruption of normal service. Any entity providing such assistance shall be reasonably compensated by the FBI pursuant to 18 U.S.C. § 3124(c) for reasonable expenses incurred in providing facilities and assistance in furtherance of the Order.

32. If **AT&T**, or any other relevant provider of electronic communication service to the public, cannot comply with this Court's Order to install the pen-trap devices, the United States requests authorization to install and use its own pen register and trap and trace devices on the network of **AT&T**, or any other relevant provider of electronic communication service to the public, pursuant to 18 U.S.C. § 3123(a)(3)(A).

33. The United States further requests that the Court order **AT&T** and any other person or entity whose assistance may facilitate execution of the Order to notify the applicant and the FBI of any changes relating to the cell phone number described in Attachment A, and to provide prior notice to the applicant and the FBI before terminating or changing service to the cell phone number.

34. The United States further requests that the Court order that the FBI and the applicant have access to the information collected by the pen-trap devices as soon as practicable, twenty-four hours per day, or at such other times as may be acceptable to them, for the duration of the Order.

35. The United States further requests, pursuant to 18 U.S.C. § 3123(d)(2), that the Court order **AT&T** and any other person or entity whose assistance facilitates execution of the Order, and their agents and employees, not to disclose in any manner, directly or indirectly, by any action or inaction, the existence of this application and Order, the resulting pen-trap devices, or this investigation, unless and until authorized by this Court, except that **AT&T** may disclose this Order to an attorney for **AT&T** for the purpose of receiving legal advice.

36. The United States further requests that this application and any resulting Order be sealed until otherwise ordered by the Court, pursuant to 18 U.S.C. § 3123(d)(1).

37. The United States further requests that the Clerk of the Court provide the United States Attorney's Office with three certified copies of this application and Order, and provide copies of this Order to the FBI and **AT&T** upon request.

38. The foregoing is based on information provided to me in my official capacity by agents of the FBI.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on October 19, 2018.

Respectfully submitted,

BENJAMIN C. GLASSMAN
United States Attorney

s/Jessica H. Kim
JESSICA H. KIM (0087831)
Assistant United States Attorney
303 Marconi Boulevard, Suite 200
Columbus, Ohio 43215
Office: (614) 469-5715
Fax: (614) 469-5653
E-mail: Jessica.Kim@usdoj.gov

ATTACHMENT A

AT&T

Facility	Number or identifier	Owner, if known	Subject of investigation, if known
Cell Phone	614-756-9477	Steven G. Rosser	Steven G. Rosser

ATTACHMENT B

THE INFORMATION TO BE DISCLOSED:

All dialing, routing, addressing, and signaling information for all calls, SMS messages, and MMS messages, as well as for all data packets associated with each electronic communication sent to or from the cell phone identified in Attachment A, including the date, time and duration of the communication and the following, without geographic limit:

- (1) Case Identification;
- (2) Intercept Access Point (IAP) System Identification;
- (3) Timestamp;
- (4) Correlation Number;
- (5) Source IP Addresses;
- (6) Destination IP Addresses;
- (7) Source Port Number;
- (8) Destination Port Number;
- (9) Transport Protocol;
- (10) Flow label (with respect to IPv6);
- (11) Packet size;
- (12) Any unique identifiers associated with cell phone devices used to make and receive calls to and from the device, and to send and receive electronic communications, including the Electronic Serial Number (“ESN”), a Mobile Equipment Identifier (“MEID”), International Mobile Station Equipment Identity (“IMEI”), or International Mobile Subscriber Identity (“IMSI”);

- (13) Source and destination telephone numbers associated with the origination and

termination of all wire and electronic communications to and from the device; and

(14) “Post-cut-through dialed digits,” which are digits dialed after the initial call set up is completed, subject to the limitations of 18 U.S.C. § 3121(c).